

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-134311

(43)公開日 平成9年(1997)5月20日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B 3 2 0 F
1/00	3 7 0		1/00	3 7 0 E
15/00	3 3 0		15/00	3 3 0 Z

審査請求 未請求 請求項の数5 O L (全 7 頁)

(21)出願番号	特願平7-289009	(71)出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(22)出願日	平成7年(1995)11月7日	(72)発明者	片岡 達史 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72)発明者	吉岡 誠 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(74)代理人	弁理士 岡田 守弘

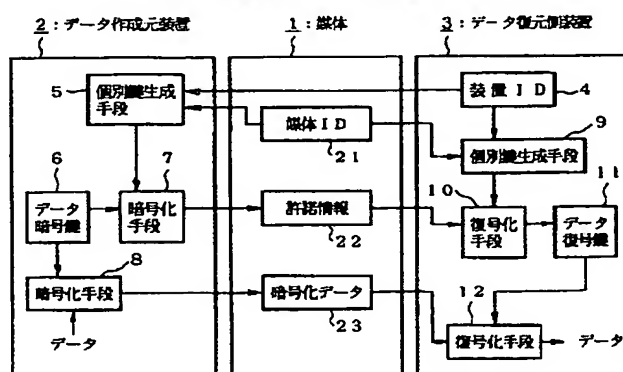
(54)【発明の名称】 機密保護システム

(57)【要約】

【課題】 本発明は、機密保護システムに関し、装置 I D、媒体 I D、データ暗号化鍵を用いて暗号化した許諾情報および暗号化データを媒体に書き込み、装置 I Dを持った装置のみが復号化可能とし、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保護を図ることを目的とする。

【解決手段】 データの書き込み時に、媒体から読み出した媒体 I Dと自身の装置 I Dとデータ暗号化鍵とから暗号化した許諾情報、およびデータ暗号鍵でデータを暗号化した暗号化データを媒体に書き込み、データの読み出し時に、媒体から読み出した媒体 I Dと許諾情報と自身の装置 I Dからデータ復号鍵を復号し、この復号したデータ復号鍵を用いて媒体から読み出した暗号化データを復号する手段を設けた装置とからなるように構成する。

本発明のシステム構成図



【特許請求の範囲】

【請求項1】媒体上のデータの機密保護する機密保護システムにおいて、

媒体ID、許諾情報、および暗号化データを書き込む可搬可能な媒体と、

データの書き込み時に、上記媒体から読み出した上記媒体IDと自身の装置IDとデータ暗号化鍵とから暗号化した許諾情報およびデータ暗号鍵でデータを暗号化した暗号化データを上記媒体に書き込み、データの読み出し時に、上記媒体から読み出した媒体IDと許諾情報と自身の装置IDからデータ復号鍵を復号し、この復号したデータ復号鍵を用いて上記媒体から読み出した暗号化データを復号する手段を設けた装置とからなることを特徴とする機密保護システム。

【請求項2】媒体上のデータの機密保護する機密保護システムにおいて、

媒体ID、許諾情報、および暗号化データを書き込む可搬可能な媒体と、

データの書き込み時に、上記媒体から読み出した上記媒体IDと自身の装置IDから生成した個別鍵でデータ暗号化鍵を暗号化した許諾情報、およびデータ暗号鍵でデータを暗号化した暗号化データを上記媒体に書き込み、データの読み出し時に、上記媒体から読み出した媒体IDと自身の装置IDから生成した個別鍵で媒体から読み出した許諾情報を復号化してデータ復号鍵を生成し、この生成したデータ復号鍵で媒体から読み出した暗号化データを復号する手段を設けた装置とからなることを特徴とする機密保護システム。

【請求項3】上記装置が複数ある場合に、装置毎の装置IDに対応して、上記許諾情報をそれぞれ生成して上記媒体にそれぞれ書き込んだことを特徴とする請求項1記載の機密保護システム。

【請求項4】上記媒体に書き込む暗号化データが複数ある場合に、暗号化データ毎に上記許諾情報を媒体に書き込むことを特徴とする請求項1記載の機密保護システム。

【請求項5】上記装置IDとしてコンピュータ装置自身の装置IDあるいは媒体に読み書きする可搬型の媒体アクセス装置の装置IDとしたことを特徴とする請求項1記載の機密保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、媒体上のデータの機密保護する機密保護システムに関するものである。

【0002】

【従来の技術】従来、複数の装置（端末）がホストに接続されたシステムにおいて、ある装置上で作成したデータをMO（光磁気ディスク）などの媒体に書き込むと共に固有識別記号を書き込んでおき、読み出す側の装置でこの固有識別記号を入力して元のデータを読み出し、媒

体が何らかの原因によって紛失したときのデータの盗用を防止していた。

【0003】

【発明が解決しようとする課題】上述したように、ある装置がデータを媒体に書き込むと共に固有識別記号を書き込んでおき、読み出し側の装置から固有識別記号を入力して媒体からデータを復元していたのでは、復元用の装置が何でもよく、復元用プログラムが媒体と一緒に盗用されてしまうと容易にデータが他の装置で復元されて非所望に使われてしまうという問題があった。

【0004】本発明は、これらの問題を解決するため、装置ID、媒体ID、データ暗号化鍵を用いて暗号化した許諾情報および暗号化データを媒体に書き込み、装置IDを持った装置のみが復号化可能とし、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保護を図ることを目的としている。

【0005】

【課題を解決するための手段】図1を参照して課題を解決するための手段を説明する。図1において、媒体1は、媒体ID、許諾情報、および暗号化データを書き込む可搬可能な媒体である。

【0006】個別鍵生成手段5は、装置ID4および媒体ID21から個別鍵を生成するものである。暗号化手段7は、データ暗号鍵6を個別鍵で暗号化して許諾情報22を生成するものである。

【0007】暗号化手段8は、データをデータ暗号鍵6で暗号化して暗号化データ23を生成するものである。個別鍵生成手段9は、装置ID4および媒体ID21から個別鍵を生成するものである。

【0008】復号化手段10は、許諾情報22を個別鍵で復号してデータ復号鍵11を生成するものである。復号化手段12は、暗号化データ23をデータ復号鍵11で復号してデータを生成するものである。

【0009】次に、動作を説明する。データの書き込み時に、個別鍵生成手段5が媒体1から読み出した媒体ID21と自身の装置ID4から生成した個別鍵でデータ暗号化鍵6を暗号化した許諾情報22を生成して媒体1に書き込むと共に、暗号化手段8がデータ暗号鍵6でデータを暗号化した暗号化データ23を媒体に書き込む。そして、データの読み出し時に、個別鍵生成手段9が媒体1から読み出した媒体ID21と自身の装置ID4から個別鍵を生成し、復号化手段10がこの生成した個別鍵で媒体1から読み出した許諾情報22を復号化してデータ復号鍵11を生成し、復号化手段12がこの生成したデータ復号鍵11で媒体1から読み出した暗号化データ23を復号しデータを生成するようにしている。

【0010】この際、装置が複数ある場合に、装置毎の装置ID4に対応して、許諾情報22をそれぞれ生成して媒体1にそれぞれ書き込むようにしている。また、

媒体 1 に書き込む暗号化データ 2 3 が複数ある場合に、暗号化データ 2 3 毎に許諾情報 2 2 を媒体 1 に書き込むようにしている。

【0011】また、装置 ID としてコンピュータ装置自身の装置 ID あるいは媒体 1 に読み書きする可搬型の媒体アクセス装置の装置 ID とするようになっている。従って、装置 ID、媒体 ID、データ暗号化鍵を用いて暗号化した許諾情報 2 2 および暗号化データ 2 3 を媒体 1 に書き込み、装置 ID を持った装置のみが復号化可能とすることにより、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保護を図ることができる。

【0012】

【発明の実施の形態】次に、図 1 から図 5 を用いて本発明の実施の形態および動作を順次詳細に説明する。

【0013】図 1 は、本発明のシステム構成図を示す。図 1 において、媒体 1 は、一意な媒体 ID、許諾情報、および暗号化データを書き込む可搬可能な媒体であって、例えば MO（光磁気ディスク）などの大容量記憶できる可搬可能な媒体である。

【0014】媒体 ID 2 1 は、媒体に書換え不可の形で一意な媒体 ID を書き込んだものであって、例えばレーザービームで所定領域に焼き切って一意の媒体 ID を書き込んだものである。これにより、媒体 1 をコピーしても当該媒体 ID がコピーできず、媒体 1 自身の偽造を防止できる。

【0015】許諾情報 2 2 は、個別鍵でデータ暗号鍵 6 を暗号化したものである。暗号化データ 2 3 は、データをデータ暗号鍵 6 で暗号化したものであって、DES などの暗号アルゴリズムで暗号化したデータである。

【0016】データ作成元装置 2 は、データ暗号鍵 6 を暗号化して媒体 1 に書き込んだり、データをデータ暗号鍵 6 で暗号して媒体 1 に書き込んだりなどするものであって、個別鍵生成手段 5、暗号化手段 7、8 などから構成されるものである。

【0017】個別鍵生成手段 5 は、媒体 1 から読み取った一意な媒体 ID 2 1 および装置 ID 4 から個別鍵を生成するものである。ここで、装置 ID としてコンピュータ装置自身の装置 ID あるいは媒体に読み書きする可搬型の媒体アクセス装置の装置 ID としている。通常は、前者を装置 ID としているが、インストール時や保守時に、可搬型の媒体アクセス装置（例えば光磁気ディスク装置）を持ち運び、制御プログラムをインストールしたり、データを格納したりするときに、1 つの当該媒体アクセス装置の装置 ID に対応づけた許諾情報および暗号化データを媒体 1 に書き込んでおけば、当該 1 台の媒体アクセス装置を用いて全ての装置へのプログラムのインストールやデータの初期設定や修正などを行うことができ、保守作業に極めて便利である。

【0018】暗号化手段 7 は、データ暗号鍵 6 を個別鍵

で暗号化して許諾情報 2 2 として媒体 1 に書き込むものである。暗号化手段 8 は、データ暗号鍵 6 でデータを暗号化し暗号化データ 2 3 として媒体 1 に書き込むものである。

【0019】データ復元側装置 3 は、データ復元側の装置であって、媒体 1 から媒体 ID、許諾情報 2 2、暗号化データ 2 3 を読み取って復号化してデータを生成するものであり、個別鍵生成手段 9、復号化手段 10、12 などから構成されるものである。

【0020】個別鍵生成手段 9 は、媒体 1 から読み取った媒体 ID と自身の装置 ID から個別鍵を生成するものである。復号化手段 10 は、生成した個別鍵で媒体 1 から読み取った許諾情報を復号化しデータ復号鍵 11 を生成するものである。

【0021】復号化手段 12 は、生成したデータ復号鍵 11 で、媒体 1 から読み取った暗号化データ 2 3 を復号してデータを生成するものである。図 2 は、本発明の媒体情報例を示す。

【0022】図 2 の (a) は、媒体情報例を示す。この媒体情報は、図 1 の可搬可能な媒体 1 に書き込む情報であって、図示の下記の情報である。

- ・媒体 ID
- ・企業固有 ID
- ・許諾情報 1 ~ n
- ・暗号化データ 1 ~ n

ここで、媒体 ID は、既述したように、レーザービームなどで媒体上に焼き切るように媒体 ID を書き込んだものであって、媒体 1 上のデータをコピーしても複製できないものである。企業固有 ID は、企業固有の ID であって、システムが異なる企業毎に一意に決定した ID である。許諾情報 1 ~ n は、装置が異なる毎に生成したものである。従って、1 つの暗号化データを n 台の装置に例えば書き込んだり、インストールしたりするには、n 個の装置毎の許諾情報を書き込むこととなる。暗号化データ 1 ~ n は、許諾情報毎の暗号化データである。尚、複数の許諾情報に対応づけて 1 つの暗号化データを格納するようにしてもよい。

【0023】図 2 の (b) は、許諾情報と装置 ID との対応づけを説明する説明図である。許諾情報は、図 1 で説明したように、装置 ID 4 と媒体 ID 2 1 から個別鍵を生成し、この個別鍵でデータ暗号鍵 6 を暗号して生成したものである。従って、結果として、装置 ID に対応づけてそれぞれ許諾情報が生成されることとなるので、その様子を模式的に表したものであり、許諾情報 1 は装置 ID 1 に対応し、以下同様に対応するものである。

【0024】次に、図 3 のフローチャートに示す順序に従い、図 1 の構成の暗号化データを作成するときの手順を詳細に説明する。図 3 は、本発明の暗号化データ作成フローチャートを示す。

【0025】図 3 において、S1 は、暗号化すべきデー

タを取り出す。S2は、データ暗号鍵を取り出す。S3は、データをデータ暗号鍵で暗号化して暗号化データを作成する。

【0026】S4は、媒体に格納する。以上によって、図1の暗号化手段8がデータ暗号鍵6を用いてデータを暗号化して生成した暗号化データ23を媒体1に書き込むことができたこととなる。

【0027】次に、図4のフローチャートに示す順序に従い、図1の構成の許諾情報を作成するときの手順を詳細に説明する。図4は、本発明の許諾情報作成フローチャートを示す。

【0028】図4において、S21は、データ復元側の装置IDを取り出す。これは、データを復元する側の装置の装置IDを取り出す。S22は、媒体IDを取り出す。これは、暗号化データを書き込もうとする媒体1から一意の媒体ID21を取り出す。

【0029】S23は、両IDにより個別鍵を作成する。これは、S21で取り出した装置IDおよびS22で取り出した媒体IDをもとに個別鍵を作成する。S24は、個別鍵でデータ暗号鍵を暗号化して許諾情報を生成する。

【0030】S25は、媒体に格納する。S26は、装置IDの数だけ繰り返したか判別する。YESの場合には、終了する。NOの場合には、S21に戻り繰り返す。

【0031】以上によって、図1の個別鍵生成手段5が復元側の装置ID4および媒体1から読み取った一意の媒体IDから個別鍵を生成し、暗号化手段7がこの個別鍵を用いてデータ暗号鍵6を暗号化して許諾情報22として媒体1に書き込むことができたこととなる。

【0032】次に、図5のフローチャートに示す順序に従い、図1の構成のデータの復号するときの手順を詳細に説明する。図5は、本発明のデータの復号化フローチャートを示す。

【0033】図5において、S31は、データ復元側の装置IDを取り出す。これは、データを復元する側の装置の装置IDを取り出す。S32は、媒体IDを取り出す。これは、暗号化データを読み出そうとする媒体1から一意の媒体ID21を取り出す。

【0034】S33は、両IDにより個別鍵を作成する。これは、S31で取り出した装置IDおよびS32で取り出した媒体IDをもとに個別鍵を作成する。S34は、媒体上の許諾情報を個別鍵を用いて復号化してデータ復号鍵を生成する。

* 【0035】S35は、媒体上の暗号化データをデータ復号鍵を用いて復号化しデータを生成する。これは、S31で復号しようとする装置から取り出した装置IDおよびS32で媒体から取り出した媒体IDから個別鍵を生成し、この個別鍵を用いて媒体1上の許諾情報を復号化してデータ暗号鍵を生成し、このデータ暗号鍵を用いて媒体1から読み出した暗号化データを復号して元のデータを生成する。

【0036】S36は、終わるか判別する。YESの場合には、終了する。NOの場合には、S34に戻り繰り返す。以上によって、図1の個別鍵生成手段9が復元側の装置の装置IDと、媒体1から読み出した媒体IDから個別鍵を生成し、復号化手段10がこの個別鍵を用いて媒体1から読み出した許諾情報を復号化してデータ復号鍵（ここではデータ暗号鍵6と同じ）を生成し、復号化手段12がこのデータ復号鍵を使って媒体1から読み出した暗号化データを復号して元のデータを生成することができたこととなる。

【0037】

【発明の効果】以上説明したように、本発明によれば、装置ID、媒体ID、データ暗号鍵を用いて暗号化した許諾情報22および暗号化データ23を媒体1に書き込み、装置IDを持った装置のみが復号化できるように構成を採用しているため、媒体1や復元プログラムが盗用されても暗号化データ23の復元を不可とし、媒体上の暗号化データの機密保護を図ることができる。

【図面の簡単な説明】

【図1】本発明のシステム構成図である。

【図2】本発明の媒体情報例である。

【図3】本発明の暗号化データ作成フローチャートである。

【図4】本発明の許諾情報作成フローチャートである。

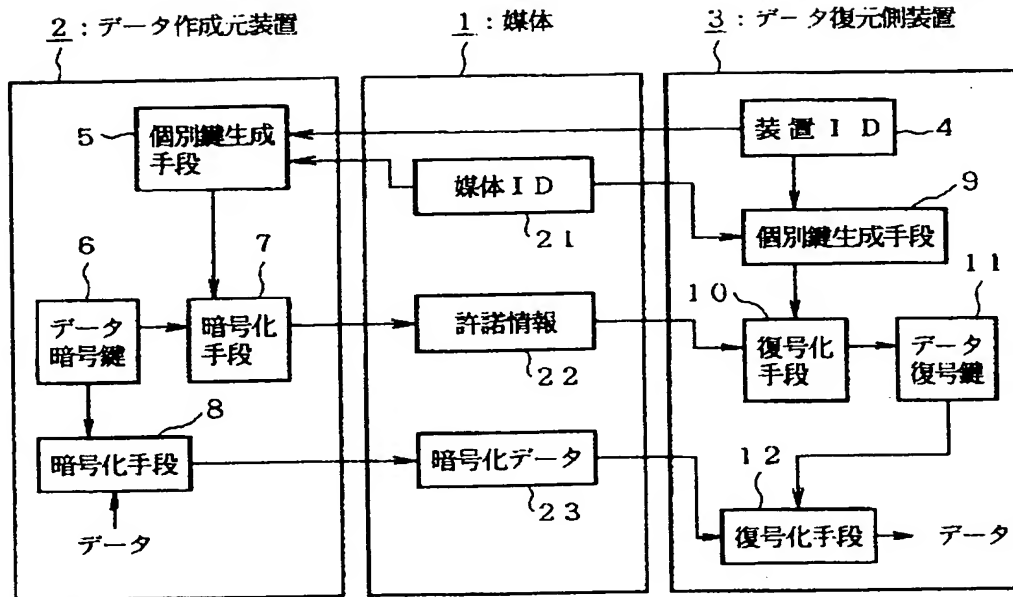
【図5】本発明のデータの復号化フローチャートである。

【符号の説明】

- 1：媒体
- 2：データ作成元装置
- 3：データ復元側装置
- 4：装置ID
- 5、9：個別鍵生成手段
- 6：データ暗号鍵
- 7、8：暗号化手段
- 10、12：復号化手段
- 11：データ復号鍵

【図 1】

本発明のシステム構成図



【図 2】

本発明の媒体情報例

(a) 媒体情報

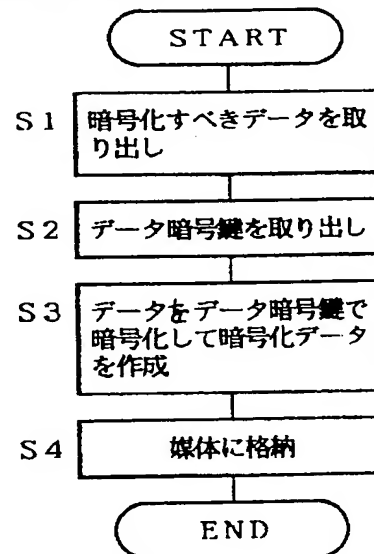
1			
媒体ID	企業固有ID	許諾情報 1 ~ n	暗号化データ 1 ~ n

(b)

許諾情報 1	← 装置ID 1
" 2	← " 2
" 3	← " 3
⋮	⋮
⋮	⋮

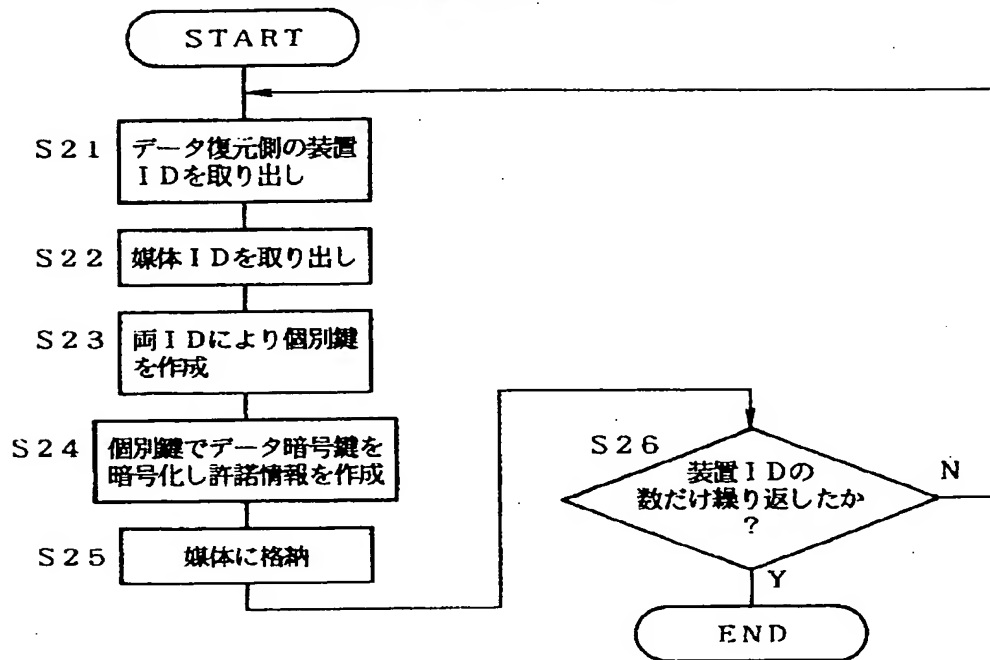
【図 3】

本発明の暗号化データ作成フローチャート



【図 4】

本発明の許諾情報作成フローチャート



【図 5】

本発明のデータの復号化フローチャート

